



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

076 952
1051
Chouanne

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le **23 JUIN 2003**

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr





26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

DS 513 W / 240899

Remise des pièces DATE 25 JUIL 2002 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0209437 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE 25 JUIL. 2002 PAR L'INPI		1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE COMPAGNIE FINANCIERE ALCATEL Département PI Sylvain CHAFFRAIX 30 avenue Kléber 75116 PARIS	
Vos références pour ce dossier (facultatif) 104745/SYC/NESO/TPM			
Confirmation d'un dépôt par télécopie <input type="checkbox"/> N° attribué par l'INPI à la télécopie			
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
<i>Demande de brevet initiale</i> <i>ou demande de certificat d'utilité initiale</i>		N°	Date <input type="text"/>
		N°	Date <input type="text"/>
Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i>		<input type="checkbox"/>	Date <input type="text"/>
		N°	Date <input type="text"/>
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) DISPOSITIF ET PROCEDE PERFECTIONNES DE TRAITEMENT DE DONNEES POUR LA GENERATION D'ALARME AU SEIN D'UN RESEAU DE COMMUNICATIONS			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation Date <input type="text"/> N° Pays ou organisation Date <input type="text"/> N° Pays ou organisation Date <input type="text"/> N° <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR		<input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»	
Nom ou dénomination sociale		ALCATEL	
Prénoms			
Forme juridique		Société Anonyme	
N° SIREN		5 . 4 . 2 . 0 . 1 . 9 . 0 . 9 . 6	
Code APE-NAF			
Adresse	Rue	54, rue La Boétie	
	Code postal et ville	75008 PARIS	
Pays		FRANCE	
Nationalité		Française	
N° de téléphone (facultatif)			
N° de télécopie (facultatif)			
Adresse électronique (facultatif)			



BREVET D'INVENTION CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

REMISE DES PIÈCES DATE 25 JUIL 2002 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0209437 NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI		CB 543 W / 255892	
Vos références pour ce dossier : <i>(facultatif)</i>			104745/SYC/NESO/TPM		
6 MANDATAIRE					
Nom			CHAFFRAIX		
Prénom			Sylvain		
Cabinet ou Société			Compagnie Financière Alcatel		
N° de pouvoir permanent et/ou de lien contractuel			PG 9222		
Adresse		Rue	30 Avenue Kléber		
		Code postal et ville	75116	PARIS	
N° de téléphone <i>(facultatif)</i>					
N° de télécopie <i>(facultatif)</i>					
Adresse électronique <i>(facultatif)</i>					
7 INVENTEUR (S)					
Les inventeurs sont les demandeurs			<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée		
8 RAPPORT DE RECHERCHE			Uniquement pour une demande de brevet (y compris division et transformation)		
Établissement immédiat ou établissement différé			<input checked="" type="checkbox"/> <input type="checkbox"/>		
Paiement échelonné de la redevance			Paiement en trois versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non		
9 RÉDUCTION DU TAUX DES REDEVANCES			Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Requête antérieurement à ce dépôt (joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence);		
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes					
10 SIGNATURE XXXXXXXXXX DU MANDATAIRE (Nom et qualité du signataire)			VISA DE LA PRÉFECTURE OU DE L'INPI L. MARIELLO		

DISPOSITIF ET PROCÉDÉ PERFECTIONNÉS DE TRAITEMENT DE DONNÉES POUR LA GÉNÉRATION D'ALARMES AU SEIN D'UN RÉSEAU DE COMMUNICATIONS

5

L'invention concerne le domaine de l'échange de données entre équipements d'un réseau de communications, et plus particulièrement celui de la gestion d'événements survenant au sein desdits équipements.

Les réseaux de communications comportent généralement un
10 dispositif de gestion de réseau (ou NMS pour « Network Management System ») censé prévenir l'opérateur lorsqu'un événement survient dans un équipement. Plus précisément, chaque fois que survient un événement au sein d'un équipement, ou dans un matériel supervisé par cet équipement, ce dernier délivre une notification représentative dudit événement. Cette
15 notification, plus connue sous l'expression anglaise « Trap » lorsque le protocole de gestion du réseau est le protocole SNMP (pour « Simple Network Management Protocol » RFC 2571-2580), est constituée de données primaires agencées selon des formats (ou protocoles) primaires. A réception de ces données primaires le gestionnaire NMS analyse leur contenu, puis s'il
20 reconnaît le premier format il génère une alarme définie par des données secondaires agencées selon un unique format (ou protocole) secondaire prédéfini.

Or, du fait de leur grande variété, les équipements d'un réseau utilisent fréquemment des formats primaires d'échange différents, difficiles,
25 voire impossibles, à modifier. Par conséquent, les gestionnaires NMS ne peuvent reconnaître qu'une partie des notifications qu'ils reçoivent.

Pour tenter de remédier à cet inconvénient, il a été proposé d'équiper le gestionnaire NMS d'un module de traitement de données primaires reposant soit sur un outil de corrélation de formats, soit sur des codes de
30 programmes, soit encore sur des fichiers de configuration. La première solution, reposant sur un outil de corrélation, met en œuvre des traitements dont la lenteur est rédhibitoire. La deuxième solution, reposant sur des codes

de programmes, nécessite des développements très coûteux. Enfin, la troisième solution n'est pas suffisamment souple pour convenir aux situations dans lesquelles les formats primaires sont assez différents, ce qui est généralement le cas. De plus, ces solutions ne permettent généralement pas
5 de synchroniser ou resynchroniser l'état d'alarme des équipements au niveau du gestionnaire NMS. Par conséquent, aucune solution proposée n'est réellement satisfaisante.

L'invention a donc pour but de remédier à tout ou partie des inconvénients précités.

10 Elle propose à cet effet un dispositif de traitement de données comportant des moyens de traitement capables de recevoir d'équipements d'un réseau de communications des données primaires (ou notification) définissant des événements dans au moins un format primaire, et de délivrer à un dispositif de gestion du réseau (ou gestionnaire NMS) des données
15 secondaires définissant des alarmes représentatives des événements, dans un format secondaire.

Ce dispositif se caractérise par le fait que ses moyens de traitement comprennent un interpréteur (ou « scripting engine ») muni de règles de conversion, agencées sous forme de « scripts » associés aux différents
20 formats primaires d'événement, et agencé de manière à convertir à l'aide de ces règles des données primaires, reçues dans l'un des formats primaires, en données secondaires dans le format secondaire interprétable par le dispositif de gestion.

Préférentiellement, l'interpréteur est agencé pour effectuer ses
25 conversions dans un format secondaire de fichier de configuration à l'aide d'un langage interprété. Plus préférentiellement encore, le format secondaire de fichier de configuration est un format de type XML (pour « eXtensible Markup Language » - version 1.0 recommandée par le W3C), et/ou le langage interprété est JavaScript (tel que défini par ECMA-262 ECMAScript :
30 A general purpose, cross-platform programming language).

Egalement de préférence, lorsque les données primaires sont respectivement associées à des identifiants d'événements, comme par exemple des identifiants d'objets (ou OID pour « Object Identifier »),

l'interpréteur peut être agencé de manière à stocker certaines au moins des règles de configuration en correspondance d'identifiants d'événements connus. Dans ce cas, l'interpréteur peut être également agencé de manière à stocker au moins une règle de conversion définissant un script par défaut
5 destiné aux données primaires qui sont associées à un identifiant d'événement inconnu.

Avantageusement, l'interpréteur peut être agencé de manière à déduire de certaines données primaires reçues (ou notification) des paramètres d'alarme lui permettant de délivrer au dispositif de gestion une
10 alarme paramétrée. Dans ce cas, les alarmes peuvent être paramétrées par des valeurs « codées en dur » et/ou extraites des données primaires, et/ou des valeurs extraites d'un équipement. Dans cette dernière hypothèse, l'interpréteur doit être agencé pour extraire d'un équipement du réseau, dont l'état d'alarme est inconnu (de préférence de sa base d'informations de
15 gestion ou MIB (pour « Management Information Base »)), des informations choisies représentatives de son état d'alarme, puis simuler l'émission de données primaires (ou notification) représentatives de ces informations d'état, de manière à générer une alarme destinée à signaler au dispositif de gestion l'état d'alarme de l'équipement.

20 Par ailleurs, les données primaires sont préférentiellement reçues dans des formats primaires de type SNMP (protocole de gestion de réseau Internet).

L'invention porte également sur un dispositif de gestion de réseau (ou gestionnaire NMS) comprenant un dispositif de traitement du type de celui
25 présenté ci-avant.

L'invention porte en outre sur un procédé de traitement de données, dans lequel, à réception de données primaires (ou notification) transmises par des équipements d'un réseau de communications et définissant des événements dans au moins un format primaire, on délivre à un dispositif de
30 gestion du réseau (ou gestionnaire NMS) des données secondaires définissant des alarmes représentatives des événements, dans un format secondaire.

Ce procédé se caractérise par le fait que son étape de génération

consiste à convertir à l'aide de règles de conversion, agencées sous forme de « scripts » associés aux différents formats primaires d'événement, des données primaires, reçues dans l'un des formats primaires, en données secondaires dans le format secondaire interprétable par le dispositif de gestion.

Le procédé selon l'invention pourra comporter de nombreuses caractéristiques complémentaires qui pourront être prises séparément et/ou en combinaison, et en particulier :

- on peut procéder à la conversion dans un format secondaire de fichier de configuration à l'aide d'un langage interprété. Il est alors préférable que le format secondaire du fichier de configuration soit un format de type XML, et/ou que le langage interprété soit JavaScript ;
- en présence de données primaires associées respectivement à des identifiants d'événements, on peut associer certaines au moins des règles de conversion à des identifiants d'événements connus. Dans ce cas, il est avantageux que l'une au moins des règles de conversion soit définie par un script par défaut destiné à des données primaires associées à un identifiant d'événement inconnu ;
- on peut déduire de certaines données primaires reçues des paramètres d'alarme, de manière à délivrer au dispositif de gestion une alarme paramétrée, par exemple par des valeurs « codées en dur » et/ou des valeurs extraites des données primaires et/ou des valeurs extraites d'un équipement ;
- on peut extraire d'un équipement du réseau, dont l'état d'alarme est inconnu, des informations choisies représentatives de son état d'alarme, puis simuler l'émission de données primaires représentatives de ces informations d'état, de manière à générer une alarme destinée à signaler au dispositif de gestion l'état d'alarme de l'équipement. Cette extraction s'effectue préférentiellement dans la base d'informations de gestion de l'équipement concerné ;
- les données primaires sont préférentiellement reçues dans des formats primaires de type SNMP.

L'invention peut notamment être mise en œuvre dans toutes les

technologies réseaux devant être gérées, et notamment dans les réseaux de transmission (par exemple de type WDM, SONET, SDH), de données (par exemple de type Internet-IP ou ATM) ou de voix (par exemple de type classique, mobile ou NGN).

5 D'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et de l'unique figure annexée qui illustre de façon schématique un exemple de réalisation d'un dispositif selon l'invention implanté dans un gestionnaire NMS d'un réseau de communications. Cette figure est, pour l'essentiel, de caractère certain. En
10 conséquence, elle pourra non seulement servir à compléter l'invention, mais aussi contribuer à sa définition, le cas échéant.

Le dispositif de traitement 1 selon l'invention est destiné à alimenter en alarmes un gestionnaire NMS (pour « Network Management System ») 2 d'un réseau de communications, par exemple de type Internet. Dans
15 l'exemple illustré sur l'unique figure, ce dispositif 1 est implanté dans le gestionnaire NMS 2, mais il pourrait être implanté dans un boîtier externe, couplé audit gestionnaire NMS.

Le réseau de communications comporte une multiplicité d'équipements de réseau 3, comme par exemple des serveurs, des
20 terminaux, des commutateurs ou des routeurs, pouvant échanger des données selon un protocole de gestion de réseau avec le gestionnaire NMS 2.

Dans ce qui suit, on considère à titre d'exemple non limitatif que le réseau de communications est de type Internet (IP) et que le protocole de
25 gestion du réseau est le protocole SNMP (pour « Simple Network Management Protocol » RFC 2571-2580). Bien entendu, l'invention s'applique à d'autres types de réseau, comme par exemple aux réseaux de transmission de type WDM, SONET ou SDH, de données de type ATM, ou de voix de type classique, mobile ou NGN, et à d'autres protocoles de gestion de réseau,
30 comme par exemple TL1 ou CORBA. Les équipements 3 du réseau sont agencés pour délivrer au gestionnaire NMS 2 des notifications (ou messages), ici de type « Trap », définies par des données primaires agencées selon un format (ou protocole) primaire, ici de type SNMP, chaque

fois que survient un événement en leur sein, ou dans un équipement ou matériel qu'ils contrôlent. Les données primaires d'une notification définissent par conséquent un événement survenu dans un équipement 3. Une multiplicité de formats primaires différents peut coexister au sein du réseau.

- 5 Par ailleurs, chaque notification est préférentiellement associée à un identifiant représentatif d'un type d'événement.

Le dispositif de traitement 1 comprend un module de traitement 4 comportant un interpréteur (ou « scripting engine ») 5 disposant d'une multiplicité de règles de conversion agencées sous la forme de « scripts »
10 associés à une multiplicité de formats primaires d'événement différents.

Plus précisément, à chaque format primaire correspond un script particulier (ou règle(s) de conversion), préférentiellement stocké dans une mémoire 6 en correspondance de l'un des identifiants d'événements contenus dans les notifications (ou Traps). Il est également préférable de prévoir au
15 moins un script par défaut pour traiter (ou initier le traitement) les données primaires agencées selon un format primaire qui est associé à un identifiant d'événement inconnu.

Ainsi, lorsqu'un interpréteur 5 reçoit une notification (ou Trap), il en extrait l'identifiant d'événement et détermine la règle de configuration (ou
20 script) stockée qui lui correspond. Il peut alors appliquer ce script (ou règle) aux données primaires définissant la notification, de manière à générer une alarme définie par des données secondaires agencées dans un langage interprété et selon un unique format secondaire interprétable par un module de contrôle 7 du gestionnaire NMS 2. En d'autres termes, les données
25 primaires reçues, agencées selon un format primaire et représentatives d'un événement, sont « converties » en données secondaires agencées selon un format secondaire et dans un langage interprété.

A réception d'une telle alarme, le module de contrôle 7 du gestionnaire NMS 2 peut alors provoquer l'affichage de l'alarme sur un écran
30 de contrôle dudit gestionnaire NMS et/ou décider d'action(s) à entreprendre dans le réseau pour tenir compte de l'alarme et/ou remédier à sa cause.

L'interpréteur 5 est agencé, à réception de données primaires, pour générer, à l'aide du script qui correspond aux données primaires reçues, une

alarme définie par des données secondaires. Dans un mode de réalisation préférentiel, ces données secondaires sont agencées sous la forme d'un fichier de configuration d'alarme selon un format (ou protocole) secondaire, de préférence de type XML (pour « eXtensible Markup Language »), et dans un langage interprété (ou « scripting language »), de préférence de type JavaScript (tel que défini par ECMA-262 ECMAScript : A general purpose, cross-platform programming language). Plus préférentiellement encore, on choisit la version 1.0, du format XML recommandée par W3C.

Bien entendu, d'autres langages interprétés (ou « scripting languages ») et d'autres formats secondaires pourraient être envisagés. Ainsi, XML peut être remplacé par des formats textes propriétaires. De même, le langage JavaScript des scripts peut être remplacé, par exemple, par VisualBasic, TCL, Perl ou encore Python.

Dans cet exemple, l'identifiant d'événement, permettant à l'interpréteur 5 de déterminer le script correspondant au format primaire des données primaires reçues, est préférentiellement de type OID (« Object Identifier » - identifiant de type simple ASN.1 permettant d'identifier un objet tel qu'un événement), dans la mesure où le langage interprété, utilisé par l'interpréteur 5 pour générer les fichiers de configuration (données secondaires), est JavaScript.

La syntaxe utilisée pour générer les fichiers de configuration d'alarme (ou données secondaires) est donc ici une combinaison de XML et de JavaScript. Plus précisément, d'une première part, la structure générale du fichier est de type XML, d'une deuxième part, les données secondaires, définissant l'alarme associée à une notification OID reçue, sont toujours encadrées par deux blocs (ou « tags ») XML, d'une troisième part, chaque champ de l'alarme possède une unique entrée, et d'une quatrième part, chaque entrée de l'alarme est soit une constante, soit une expression JavaScript.

Ainsi, lorsque toutes les entrées de l'alarme sont des constantes, le fichier de configuration d'alarme est principalement de type XML. Par exemple, il se présente sous la forme <SEVERITY>Critical</SEVERITY>. Lorsque certaines au moins des entrées de l'alarme sont des expressions

JavaScript, un maximum de souplesse peut être obtenu. Le fichier se présente alors, par exemple, sous la forme <SEVERITY>(trapget(« 1.2.3.4 »)==2) ? Critical : Major</SEVERITY>.

5 Certains champs de l'alarme générée peuvent être optionnels ou présenter une valeur par défaut.

Grâce aux scripts, il est possible de tirer pleinement partie des informations contenues dans les données primaires qui constituent les notifications reçues. De nombreux traitements, notamment logiques et/ou calculatoires, peuvent être ainsi appliqués aux paramètres qui définissent les événements signalés par les équipements 3 du réseau. Par conséquent, l'interpréteur 5 peut non seulement générer une alarme représentative d'un événement, mais également accompagner cette alarme de paramètres (ou de valeurs de paramètres) susceptibles d'en faciliter le traitement au niveau du gestionnaire NMS 2.

15 Les alarmes peuvent ainsi être paramétrées par des valeurs « codées en dur » et/ou extraites de la notification (ou Trap) et/ou extraites d'un équipement dont on a reçu une notification (ou Trap).

Afin de mettre en œuvre cette troisième possibilité, l'interpréteur 5 doit être agencé de manière à adresser à un équipement, dont il a éventuellement reçu des données primaires représentatives d'un état d'alarme inconnu, un message requérant de sa part certaines informations susceptibles de permettre la détermination dudit état d'alarme. Généralement, ces informations sont contenues dans la base d'informations de gestion 8 (ou MIB pour « Management Information Base ») de l'équipement 3.

25 Grâce à cet agencement lui permettant d'extraire des informations d'un équipement 3 distant, et notamment de sa MIB 8, le dispositif selon l'invention 1 peut assurer une fonction de synchronisation et resynchronisation de l'état d'alarme de chaque équipement. En effet, chaque fois que le gestionnaire NMS du réseau 2 (ou son dispositif de traitement 1) est redémarré ou déconnecté du reste du réseau, par exemple en cas de panne ou d'intervention de maintenance, il doit être, d'une part, resynchronisé par rapport aux états d'alarmes respectifs des équipements 3 du réseau qui étaient présents au moment de sa déconnexion, lesquels états ont pu

évoluer, et d'autre part, synchronisé par rapport aux états d'alarmes respectifs des nouveaux équipements 3 du réseau, lesquels états lui sont inconnus. Il en va de même chaque fois qu'un nouvel équipement 3 se connecte au réseau ou qu'un ancien équipement se reconnecte au réseau.

5 Cette fonction peut être assurée par une ou plusieurs règles, par exemple stockées dans la mémoire 6, soit automatiquement lors de chaque mise en fonctionnement et/ou chaque fois que l'interpréteur 5 est averti d'une (re)connexion par le module de contrôle 7 du gestionnaire NMS 2 du réseau, soit semi-automatiquement chaque fois que la personne responsable de la
10 gestion du réseau en donne l'ordre à l'interpréteur 5.

La ou les règles de (re)synchronisation sont agencées pour examiner le contenu de la MIB du ou des équipements 3 désignés, de manière à extraire les informations (paramètre(s) ou valeur(s) de paramètre(s)) définissant leur(s) état(s) d'alarme. Mais, ces règles peuvent également servir
15 à vérifier ou contrôler la valeur d'un ou plusieurs paramètres. Comme indiqué ci-dessus, dans certaines situations tous les équipements du réseau, qui dialoguent avec le gestionnaire NMS 2, peuvent faire l'objet d'un examen à l'aide des règles de (re)synchronisation.

La ou les règles de (re)synchronisation peuvent être agencées de
20 manière à simuler l'émission d'une notification (ou Trap) à l'intérieur du gestionnaire NMS 2. Plus précisément, elles indiquent les notifications (ou Traps) que l'équipement 3 aurait dû envoyer pour passer d'un état sans alarme à son état en cours. Ces notifications (ou Traps) simulées font ensuite l'objet d'une conversion semblable à celle appliquée aux notifications réelles.

25 Le module de traitement 4 du dispositif 1, et son interpréteur 5, peuvent être respectivement réalisés sous la forme de circuits électroniques, de modules logiciels (ou informatiques), ou d'une combinaison de circuits et de logiciels.

L'invention offre également un procédé de traitement de données,
30 dans lequel, à réception de données primaires transmises par des équipements 3 d'un réseau de communications et définissant des événements dans au moins un format primaire, on délivre à un dispositif de gestion du réseau 2 (ou gestionnaire NMS) des données secondaires qui

définissent des alarmes représentatives de ces événements, dans un format secondaire.

5 Celui-ci peut être mis en œuvre à l'aide du dispositif de traitement présenté ci-avant. La fonction principale et les sous-fonctions optionnelles assurées par les étapes de ce procédé étant sensiblement identiques à celles assurées par les différents moyens constituant le dispositif de traitement 1, seule sera résumée ci-après l'étape mettant en œuvre la fonction principale du procédé selon l'invention.

10 Ce procédé se caractérise par le fait que son étape de génération consiste à convertir à l'aide de règles de conversion, agencées sous forme de « scripts » associés aux différents formats primaires d'événement, des données primaires, reçues dans l'un des formats primaires, en données secondaires dans le format secondaire interprétable par le dispositif de gestion 2.

15 Grâce à l'invention, il n'est plus nécessaire de recourir à la programmation, ce qui permet de réduire les coûts de développement. De plus, les scripts procurent une grande souplesse d'utilisation et une grande rapidité de traitement (plusieurs dizaines de notifications (ou Traps) par seconde), et permettent une adaptation rapide à tous les types de formats
20 primaires. En outre, l'invention permet une (re)synchronisation.

L'invention ne se limite pas aux modes de réalisation de procédé et dispositifs décrits ci-avant, seulement à titre d'exemple, mais elle englobe toutes les variantes que pourra envisager l'homme de l'art dans le cadre des revendications ci-après.

REVENDEICATIONS

1. Dispositif de traitement de données (1) comportant des moyens de
5 traitement (4) propres à recevoir d'équipements (3) d'un réseau de
communications des données primaires définissant des événements dans au
moins un format primaire, et à délivrer à un dispositif de gestion dudit réseau
(2) des données secondaires définissant des alarmes représentatives desdits
10 événements, dans un format secondaire, caractérisé en ce que lesdits
moyens de traitement (4) comprennent un interpréteur (5) muni de règles de
conversion, agencées sous forme de « scripts » associés aux différents
formats primaires d'événement, et agencé pour convertir à l'aide desdites
règles des données primaires, reçues dans l'un desdits formats primaires, en
données secondaires dans ledit format secondaire interprétable par ledit
15 dispositif de gestion (2).

2. Dispositif selon la revendication 1, caractérisé en ce que ledit
interpréteur (5) est agencé pour effectuer lesdites conversions dans un format
secondaire de fichier de configuration à l'aide d'un langage interprété.

3. Dispositif selon la revendication 2, caractérisé en ce que ledit format
20 secondaire de fichier de configuration est un format choisi dans un groupe
comprenant XML et les formats textes propriétaires.

4. Dispositif selon l'une des revendications 2 et 3, caractérisé en ce
que ledit langage interprété est choisi dans un groupe comprenant au moins
JavaScript, VisualBasic, TCL, Perl et Python.

25 5. Dispositif selon l'une des revendications 1 à 4, caractérisé en ce
que, en présence de données primaires associées respectivement à des
identifiants d'événements, ledit interpréteur (5) est agencé pour stocker
certaines au moins desdites règles en correspondance d'identifiants
d'événements connus.

30 6. Dispositif selon la revendication 5, caractérisé en ce que ledit
interpréteur (5) est agencé pour stocker au moins une règle de conversion
définissant un script par défaut destiné aux données primaires associées à un
identifiant d'événement inconnu.

7. Dispositif selon l'une des revendications 1 à 6, caractérisé en ce que ledit interpréteur (5) est agencé pour déduire de certaines données primaires reçues des paramètres d'alarme, de manière à délivrer audit dispositif de gestion (2) une alarme paramétrée.

5 8. Dispositif selon la revendication 7, caractérisé en ce que ledit interpréteur (5) est agencé pour délivrer au dit dispositif de gestion (2) des alarmes paramétrées par des valeurs « codées en dur ».

9. Dispositif selon l'une des revendications 7 et 8, caractérisé en ce que ledit interpréteur (5) est agencé pour délivrer audit dispositif de gestion (2)
10 des alarmes paramétrées par des valeurs extraites desdites données primaires.

10. Dispositif selon l'une des revendications 1 à 9, caractérisé en ce que, lorsque l'état d'alarme d'un équipement (3) du réseau est inconnu, ledit interpréteur (5) est agencé pour extraire dudit équipement (3) des
15 informations choisies représentatives dudit état d'alarme, puis simuler l'émission de données primaires représentatives desdites informations d'état, de manière à générer une alarme destinée à signaler au dispositif de gestion (2) l'état d'alarme dudit équipement (3).

11. Dispositif selon la revendication 10 en combinaison avec l'une des
20 revendications 7 à 9, caractérisé en ce que ledit interpréteur (5) est agencé pour délivrer audit dispositif de gestion (2) des alarmes paramétrées par des valeurs extraites de l'équipement duquel il a reçu des données primaires.

12. Dispositif selon l'une des revendications 10 et 11, caractérisé en ce que ledit interpréteur (5) est agencé pour extraire lesdites informations ou
25 valeurs d'une base d'informations de gestion (8) de l'équipement concerné.

13. Dispositif selon l'une des revendications 1 à 12, caractérisé en ce que lesdites données primaires sont reçues dans des formats primaires de type SNMP.

14. Dispositif de gestion de réseau (2), caractérisé en ce qu'il comprend
30 un dispositif de traitement (1) selon l'une des revendications précédentes.

15. Procédé de traitement de données, dans lequel, à réception de données primaires transmises par des équipements (3) d'un réseau de communications et définissant des événements dans au moins un format

primaire, on délivre à un dispositif de gestion du réseau (2) des données secondaires définissant des alarmes représentatives desdits événements, dans un format secondaire, caractérisé en ce que ladite génération consiste à convertir à l'aide de règles de conversion, agencées sous forme de « scripts » associés aux différents formats primaires d'événement, des données primaires, reçues dans l'un desdits formats primaires, en données secondaires dans ledit format secondaire interprétable par ledit dispositif de gestion (2).

16. Procédé selon la revendication 15, caractérisé en ce que l'on procède à la conversion dans un format secondaire de fichier de configuration à l'aide d'un langage interprété.

17. Dispositif selon la revendication 16, caractérisé en ce que ledit format secondaire de fichier de configuration est un format choisi dans un groupe comprenant XML et les formats textes propriétaires.

18. Dispositif selon l'une des revendications 16 et 17, caractérisé en ce que ledit langage interprété est choisi dans un groupe comprenant au moins JavaScript, VisualBasic, TCL, Perl et Python.

19. Procédé selon l'une des revendications 15 à 18, caractérisé en ce que, en présence de données primaires associées respectivement à des identifiants d'événements, on associe certaines au moins desdites règles de conversion à des identifiants d'événements connus.

20. Procédé selon la revendication 19, caractérisé en ce que l'une au moins desdites règles de conversion définit un script par défaut destiné à des données primaires associées à un identifiant d'événement inconnu.

21. Procédé selon l'une des revendications 15 à 20, caractérisé en ce que l'on déduit de certaines données primaires reçues des paramètres d'alarme, de manière à délivrer audit dispositif de gestion (2) une alarme paramétrée.

22. Procédé selon la revendication 21, caractérisé en ce que l'on délivre audit dispositif de gestion (2) des alarmes paramétrées par des valeurs « codées en dur ».

23. Procédé selon l'une des revendications 21 et 22, caractérisé en ce que l'on délivre audit dispositif de gestion (2) des alarmes paramétrées par

des valeurs extraites desdites données primaires.

24. Procédé selon l'une des revendications 15 à 23, caractérisé en ce que, lorsque l'état d'alarme d'un équipement (3) du réseau est inconnu, on extrait dudit équipement (3) des informations choisies représentatives dudit état d'alarme, puis on simule l'émission de données primaires représentatives desdites informations d'état, de manière à générer une alarme destinée à signaler au dispositif de gestion (2) l'état d'alarme dudit équipement (3).

25. Procédé selon la revendication 24 en combinaison avec l'une des revendications 21 à 23, caractérisé en ce que l'on délivre audit dispositif de gestion (2) des alarmes paramétrées par des valeurs extraites de l'équipement (3) duquel il a reçu des données primaires.

26. Procédé selon l'une des revendications 24 et 25, caractérisé en ce que l'on extrait lesdites informations ou valeurs d'une base d'informations de gestion (8) de l'équipement (3) concerné.

27. Procédé selon l'une des revendications 15 à 26, caractérisé en ce que lesdites données primaires sont reçues dans des formats primaires de type SNMP.

28. Utilisation des procédé, dispositif de traitement (1) et dispositif de gestion (2) selon l'une des revendications précédentes dans les technologies réseaux devant être gérées.

29. Utilisation selon la revendication 28, caractérisé en ce que lesdites technologies réseaux sont choisies dans un groupe comprenant les réseaux de transmission, en particulier de type WDM, SONET et SDH, de données, en particulier de type Internet-IP et ATM, et de voix, en particulier de type classique, mobile et NGN.

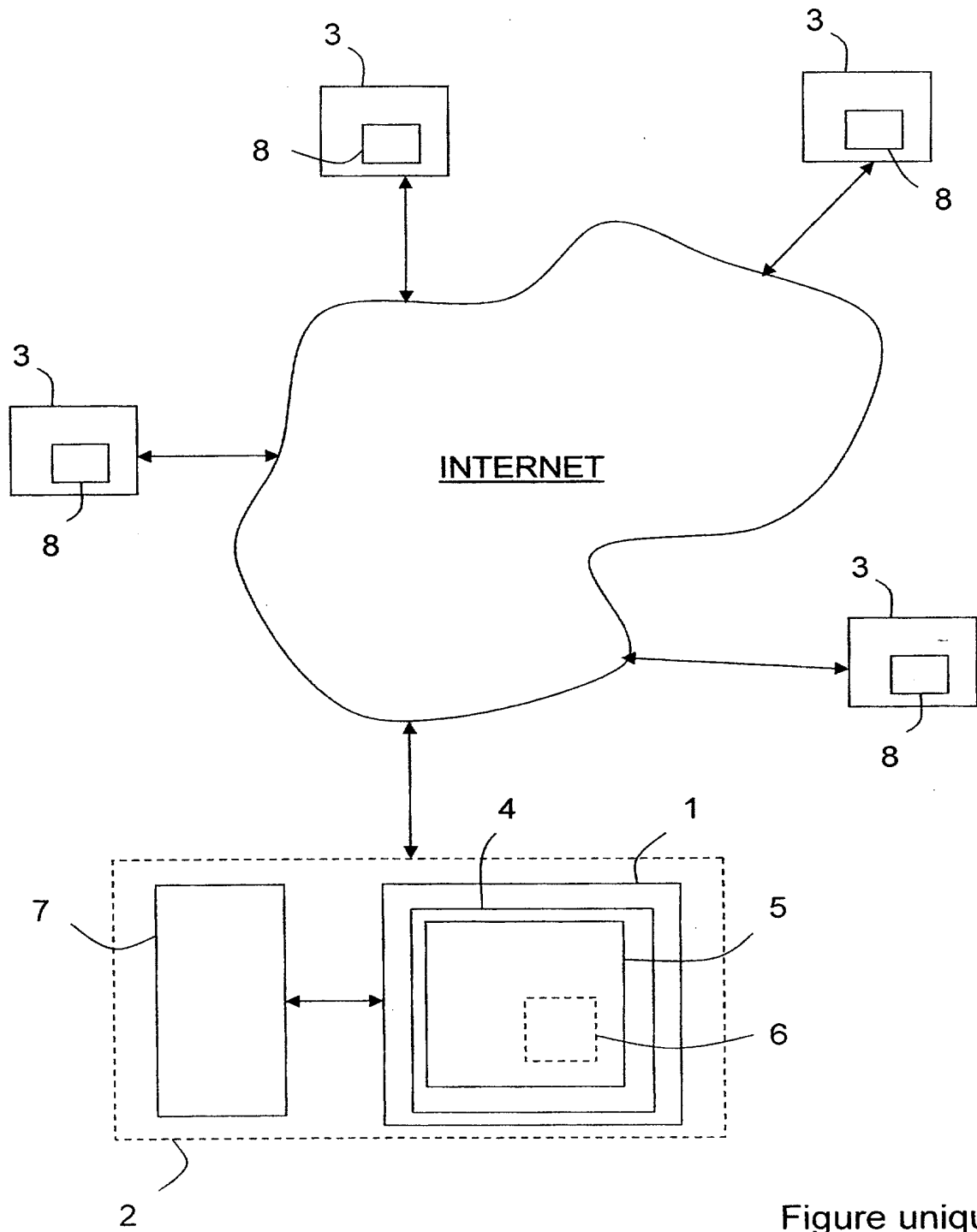


Figure unique



DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg

75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 1. / 1.

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

CB 113 W 1260891

Vos références pour ce dossier <i>(facultatif)</i>		104745/SYC/NESO/TPM	
N° D'ENREGISTREMENT NATIONAL		0205437 2	
TITRE DE L'INVENTION (200 caractères ou espaces maximum) DISPOSITIF ET PROCEDE PERFECTIONNES DE TRAITEMENT DE DONNEES POUR LA GENERATION D'ALARMES AU SEIN D'UN RESEAU DE COMMUNICATIONS			
LE(S) DEMANDEUR(S) : Société anonyme ALCATEL			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		CHEVANNE	
Prénoms		Michel	
Adresse	Rue	135, RUE D'ALÉSIA	
	Code postal et ville	75014	PARIS, FRANCE
Société d'appartenance <i>(facultatif)</i>			
Nom		LAPRAYE	
Prénoms		Bertrand	
Adresse	Rue	CHATEAU DE COURCELLE 158, AVENUE DU GÉNÉRAL LECLERC	
	Code postal et ville	91190	GIF SUR YVETTE, FRANCE
Société d'appartenance <i>(facultatif)</i>			
Nom		DRUGMAND	
Prénoms		Philippe	
Adresse	Rue	21, RUE DES ORMEAUX	
	Code postal et ville	92260	FONTENAY AUX ROSES, FRANCE
Société d'appartenance <i>(facultatif)</i>			
DATE ET SIGNATURE(S) XXXXX XXXXX DU MANDATAIRE (Nom et qualité du signataire)		23 juillet 2002 Sylvain CHAFFRAIX 	





12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200